Transactions of the Korean Nuclear Society Spring Meeting
Jeju, Korea, May 18-19, 2017

Application Study for Implementing IEEE 1012-2016

Jin-Ku Kim, Jin-Beom Woo, Se-Jun Kim, Hyun-Woo Kim, You-Sung Ro, Jong-Jae, Choi, Jae-Hyuk Park*
KEPCO Engineering & Construction, Inc., 269, Hyeoksin-ro, Gimcheon-si, Gyeongsangbuk-do, South Korea
**Corresponding author: jaehpark@kepco-enc.com*

1. Introduction

Over the past 9 years the US NRC has endorsed various versions of IEEE 1012 through Regulatory Guide (RG) 1.168 "Verification, Validation, Reviews, And Audits For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants." The first release of this regulatory guide was in 1997 which endorsed IEEE 1012-1986. The next revision of RG 1.168 was issued in 2004 and it endorsed IEEE 1012-1998. The current revision of RG 1.168 issued in 2013 endorses IEEE 1012-2004. Since that latest US NRC endorsement in 2013, IEEE 1012-2004 has been the industry benchmark for software verification and validation (V&V) activities.

While draft version IEEE 1012-2016 is the latest version of IEEE 1012, that version is being issued primarily to align the IEEE terminology and structure more completely with the terminology and structure of corresponding International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) documents.

This paper provides the recommendations for compliance with IEEE 1012-2016 "Draft Standard for System, Software and Hardware Verification and Validation", January 2016.

2. Key Changes from IEEE 1012-2004 to IEEE 1012-2012

IEEE 1012-2004 was limited to software V&V. IEEE1012-2012 expands the scope to encompass hardware and systems. As such the term "software integrity level" has been changed to "integrity level" and most references to software have been changed to system. All discussion of "components" is expanded from software to software and hardware components. V&V tasks are categorized by software, hardware and system; tasks that are applicable to all aspects are categorized as "common". Each category defines the applicable tasks for each integrity level.

2.1 Integrity Levels (Section 5)

In IEEE 1012-2012 the integrity levels are used only to define a graded approach to the rigor of V&V. As the integrity level decreases, so does the required scope, intensity, and degree of rigor associated with the V&V tasks.

It is noted that IEEE 1012-2012 does not require the same integrity level to be used for all the subsystems or elements of the system of interest. IEEE 1012-2004 is silent on this issue. As a result, this has been a point of disagreement between industry and US NRC; US NRC expects all elements of a system to be the same integrity level.

2.2 V&V Processes Overview (Section 6)

IEEE 1012-2004 permits the V&V organization to conduct V&V for tests specified, performed and documented by the design organization. But IEEE1012-2012 requires the V&V organization to "perform" the testing for integrity levels 3 and 4. IEEE 1012-2012 explains the merits of tests specified from the diverse and independent perspective of the V&V organization, rather than the design organization.

2.3 V&V Comparison IEEE 1012-2012 to IEEE 1012-2004

This section compares the software V&V activities in IEEE 1012-2004 to the common, system, software, and hardware V&V activities in IEEE 1012-2012. This comparison is summarized in the Table 1.

Table 1: Comparison IEEE 1012-2012 to 2004

V&V Activity Title Comparisons				
2004 Software V&V	**2012**			
	Common V&V	**System V&V**	**Software V&V**	**Hardware V&V**
X = Equivalent title to 2004 software V&V (may have minor word changes)				
Management	X			
Acquisition	X			
Supply Planning	X			
	Project Planning			
	Conf. Manag.			
Concept			X	X
Requirements		Requir. Definition	X	X
		Requir. Analysis		
Design		Archit. Design	X	X
Implement		X	Construct	Fabrication
Test		Integration	Integ. Test	Integ. Test
			Qual. Test	Qual. Test
			Acc. Test	Acc. Test
Installation, Checkout		Transition	X	Transition
Operation		X	X	X
Maintenance		X	X	X
		Disposal	Disposal	Disposal

3. Key Changes from IEEE 1012-2012 to IEEE 1012-2016

The overview, definitions, integrity levels and V&V process overview are essentially unchanged between IEEE 1012-2012 and IEEE 1012-2016. There are a few additional definitions that are insignificant.

Table 2: Comparison IEEE 1012-2012 to 2016

V&V Activity Title Comparisons				
2004 Software V&V	**2012 with 2016 changes in red, bold text**			
	Common V&V	**System V&V**	**Software V&V**	**Hardware V&V**
X = Equivalent title to 2004 software V&V (may have minor word changes)				
Management	X			
Acquisition	X			
Supply Planning	X			
	Project Planning			
	Conf. Manag.			
Concept			X	X
Requirements		**Business or Mission Analysis**	X	X
		Stakeholder **Needs and** Requirements Definition		
		System Requir. **Definition**		
Design		Architectural **Definition**	X	X
		Design Definition		
		System Analysis		
Implementation		X	Construction	Fabrication
Test		Integration	Integration	Integration
			Qualification Testing	Qualification Testing
			Accept. Testing	Acceptance Testing
		Verification	**Verification**	**Verification**
Installation, Checkout		Transition	X	Transition
		Validation	**Validation**	**Validation**
Operation		X	X	X
Maintenance		X	X	X
		Disposal	Disposal	Disposal

The Table 2 above identifies the software V&V activity changes from IEEE 1012-2012 to 2016, using the same Table 1 as in Section 2.3 above. Changes from IEEE 1012-2012 to 2016 are in **bold red** text

4. Technology Plan of System V&V

All System V&V activities provide assurance that the outcomes of the system level processes in ISO/IEC/IEEE 15288-2015 have been achieved. These system level processes in ISO/IEC/IEEE 15288-2015 have the same titles as the System V&V Activities shown in the Table 2 of Section 3, above.

It is noted that system related V&V activities are defined as separate system activities in ISO/IEC/IEEE 15288-2015. But since the tasks for these activities are defined by the other System V&V activities within the System V&V section, IEEE 1012-2016 does not define any unique tasks for the System V&V activities.

5. Technology Plan of software V&V

Performing software integration tests and documenting software integration test results are Software V&V subtasks under the Software Integration V&V activity. Performing software qualification tests and documenting qualification test results are Software V&V subtasks under the Software Qualification Testing V&V activity. Similarly, performing software acceptance tests and documenting acceptance test results are software V&V subtask under the Software Acceptance Testing V&V activity. For integrity levels 4 and 3 these tests are conducted by the V&V organization. For integrity level 2, these tests can be conducted by the design organization and reviewed by the V&V organization.

6. Technology Plan of Hardware V&V

All Hardware V&V activities provide assurance that the outcomes of various hardware processes have been achieved, including the system architectural design process in ISO/IEC 12207-2008.

It is noted that hardware related V&V activities are defined by the other Hardware V&V activities within the Hardware V&V section. Therefore, IEEE 1012-2016 does not define any unique tasks for the Hardware V&V activities.

7. Conclusions

Unlike these relatively minor changes from the IEEE 1012-2012 version to the IEEE 1012-2016 version, the change from the IEEE 1012-2004 to the IEEE 1012-2012 version was much more significant. The IEEE 1012-2012 revision expanded the scope of the V&V processes to include systems and hardware, as well as software. The standard was restructured to allow for the performance of system, software, and hardware V&V individually or in any combination. The standard also contains separate clauses that address common, system, software, and hardware V&V activities.

Since the US NRC has not yet endorsed IEEE 1012-2012, it has not been adopted by the nuclear industry. Most suppliers and utilities continue to follow the guidance in the US NRC endorsed version of IEEE 1012, which is the 2004 version. But US NRC endorsement of the IEEE 1012-2012 version is inevitable, and is likely to occur as early as 2017. Therefore, compliance to IEEE 1012-2012 represents the most significant change for the nuclear industry; the new terminology changes of IEEE 1012-2016 are quite minor.

REFERENCES

[1] Regulatory Guide 1.168 “Verification, Validation, Reviews, And Audits For Digital Computer Software Used In Safety Systems Of Nuclear Power Plants”.
[2] ISO/IEC/IEEE 15288-2015 “System and Software Engineering – System Life Cycle Processes”.
[3] ISO/IEC/IEEE 12207-2008 “System and Software Engineering – System Life Cycle Processes”.